REMARKS/ARGUMENTS

Applicant respectfully requests reconsideration of this application in view of the following remarks.

Claim 1, claim 14, and claim 22 have been amended to more particularly point out Applicant's invention. No new matter has been added.

Claim Rejection under 35 U.S.C. § 102(e)

The Office at 5 states:

5. Claims 1-4, 10, 12, 14-16 and 22-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Purtell et al U.S. Patent No. 6,950,947 B1.
(Emphasis in original.)

Claims 1, 14, and 22 Rejection under 35 U.S.C. § 102(e) - Purtell

The Office at 5 states:

As to claims 1, 14 and 22, Purtell et al discloses a method for traversing a firewall, comprising:

> initiating a first connection to go through the firewall [column 7 line 18 to column 8 line 62];
>
> evaluating the first connection for a response from a remote system indicating a successful first connection [column 7 line 18 to column 8 line 62];
>
> initiating a second connection to go through the firewall if a successful first connection is not established [column 7 line 18 to column 8 line 62];
>
> evaluating the second connection for a response from a remote system indicating a successful second connection [column 7 line 18 to column 8 line 62];
>
> initiating a third connection to go through the firewall if a successful second connection is not established [column 7 line 18 to column 8 line 62]; and

evaluating the third connection for a response from a remote system indicating a successful third connection [column 7 line 18 to column 9 line 62].

The cited reference states in part:

Referring to FIG. 5, a process is shown for using a CCB 300 when opening a connection from a firewall 100 to an external network 110. In step 500, the firewall 100 receives an instruction from a particular client 112 to retrieve data, such as a web page, from a specific external server 114. The firewall 100 determines if a CCB 300 already exists that contains shared connection state data 306 for a TCP connection between the firewall 100 and the specific server 114. The presence or absence of such a CCB 300 will affect the actions taken by the firewall 100 to connect to the server 114. Next, in step 502, the firewall 100 sends a SYN flag to the specific server 114. SYN is a common abbreviation for synchronize, and is a standard TCP command for initiating a connection between a client and a server. In the next step 504, the firewall 100 determines whether a SYN and an ACK have been received back from the specific server 114. ACK stands for acknowledge, and is a flag indicating that a SYN flag sent from a first computer has been received by a second computer. The SYN flag that is sent from the server 114 back to the firewall 100 represents the attempt by the server 114 to open a connection back to the firewall 100. The response of SYN and ACK to a SYN flag is part of the TCP standard, and is well known to those skilled in the art. In step 506, if the particular server 114 has returned a SYN and ACK to the firewall 100, the firewall 100 updates the CCB 300 with the state information associated with the state of the connection between the firewall 100 and the server 114 as determined from the packet or packets containing the SYN and ACK flags. The firewall 100 then transmits an ACK to the server 114, as expected in the TCP standard, to open the other end of the connection.

However, if no SYN and ACK are received from the server 114 in step 504, the process proceeds to step 508. In step 508, the firewall 100 determines whether an RST flag has been received from the particular server 114. RST is an abbreviation for reset, and is a standard TCP command issued from a server to a client after receiving a SYN flag when the server detects a half-open connection or other anomaly. The RST flag is a well-known part of the TCP standard, and its use is well known to those skilled in the art. If the firewall 100 has received an RST flag from the particular server 114, then the process proceeds to step 510, where the firewall updates the CCB 300 with the state information associated with the state of the connection between the firewall 100 and the server 114, as determined from the packet or packets

containing the RST flag. The firewall 100 then considers the connection attempt rejected. However, in step 508, if no RST flag is received from the particular server 114, the firewall 100 continues to wait for a fixed period of time for a response from the server 114. This fixed period of time is preferably substantially equal to the round trip time (RTT) estimate. Preferably, if a CCB 300 exists for the connection, then the RTT contained within the CCB is used. If no response is received from the server 114 after that fixed period of time, **retransmission preferably may be attempted up to twelve times**, using exponentially increasing but bounded waiting periods. For example, the waiting periods may be two times the RTT, then four times the RTT, then eight times the RTT, and so on, up to the upper bound. If no connection is established, the client 112 is notified by the firewall 100 that the connection attempt with the particular server 114 was unsuccessful. No connection is established. .

(Emphases added.)

Applicant submits that Purtell et al ("Purtell") in the cited section and Figure 5 discloses a firewall 100 receiving an instruction from a client 112 behind the firewall to retrieve data from a server 114 outside the firewall 100. The firewall computer 100 checks for a control block 500, and then sends a single type connection request (SYN) for a connection 502 to a server 114. If the request is acknowledged 504 then the control block is updated 506 and a connection is established 516, communication occurs and when done the connection is shut down 520, the control block is updated 522 and the connection closed 524.

If on the other hand the single type connection request (SYN) for a connection 502 to a server 114 is NOT acknowledged then a check is made to see if a reset command was received 508 and if so then the control block 510 is updated immediately otherwise a timeout 512 occurs and multiple retransmission attempts may be made before the control block 510 is updated, then the connection is closed 514.

As amended, Applicant's independent claims 1, 14, and 22 recite

"wherein said second connection is different than said first connection" and "wherein said third connection is different than said second connection and said first connection". (Emphases added.)

NOWHERE in Purtell is there any mention of a second, much less a third connection attempt as Applicant has claimed wherein the connections are different thusly, citing from claim 1:

...

initiating a second connection to go through said firewall if a successful first connection is not established, wherein said second connection is different than said first connection;

evaluating the second connection for a response from a remote system indicating a successful second connection;

initiating a third connection to go through said firewall if a successful second connection is not established, wherein said third connection is different than said second connection and said first connection; and

evaluating the third connection for a response from a remote system indicating a successful third connection.

(Emphases added.)

Applicant respectfully asserts that a *prima facie* rejection of claims 1, 14, and 22 under 35 U.S.C. § 102 based upon Purtell should be withdrawn. In order to establish a *prima facie* rejection under 35 U.S.C. § 102, the United States Patent & Trademark Office (USPTO) must provide a "single prior art reference [in which] disclosure of each and every element of the claimed invention, *arranged as in the claim* [exists in the reference]." *Lindemann Maschinenfabrik v. American Hoist & Derrick* ("*Lindemann*"), 730 F.2d 1452, 1458 (Fed. Cir. 1984) (Emphases added). Additionally, each and every element of the claim must be *exactly* disclosed in the anticipatory reference. *Titanium Metals Corp. of America v. Banner*, 778 F.2d 775, 777 (Fed. Cir. 1985).

Applicant submits that because Purtell fails to disclose a second and third connections that are each different, that Purtell fails to anticipate what Applicant has

claimed. Applicant respectfully requests allowance of independent claims 1, 14, and 22; and claims 2-4, 10, 12, 15, 16, and 23-26 which are dependent on these independent claims.

Claims 2, 15, and 23 Rejection under 35 U.S.C. § 102(e) - Purtell

The Office at 5 states:

> As to claims 2, 15 and 23, Purtell et al discloses that the first connection, the second connection, and the third connection is selected from the group consisting of Transmission Control Protocol (TCP) connection, User Datagram Protocol (UDP) connection, hypertext transfer protocol (HTTP) connection, hypertext transfer protocol (HTTP) connection via a proxy connection, and Internet Control Message Protocol (ICMP) connection [column 3 line 51 to column 4 line 11].

As amended, Applicant's independent claim 1, claim 14, and claim 22 now recite a limitation wherein the second connection is different than the first connection and the third connection is different than the second connection and the first connection upon which dependent claim 2, claim 15, and claim 23 respectively depend. Applicant submits that because Purtell fails to disclose a second and third connections that are each different, that Purtell fails to anticipate what Applicant has claimed. Applicant respectfully requests allowance of dependent claims 2, 15, and 23.

The additional limitations in claims 2, 15, and 23 are also not anticipated. Applicant respectfully requests allowance of claims 2, 15, and 23.

Claim 3 Rejection under 35 U.S.C. § 102(e) - Purtell

The Office at 5 states:

As to claim 3, Purtell et al discloses that initiating a TCP connection comprises initiating a TCP connection to a predefined address and port [column 3 line 51 to column 4 line 11].

As amended, Applicant's independent claim 1 now recites a limitation wherein the second connection is different than the first connection and the third connection is different than the second connection and the first connection upon which dependent claim 3 depends. Applicant submits that because Purtell fails to disclose a second and third connections that are each different, that Purtell fails to anticipate what Applicant has claimed. Applicant respectfully requests allowance of dependent claim 3.

The additional limitation in claim 3 is also not anticipated. Applicant respectfully requests allowance of claim 3.

Claim 10 Rejection under 35 U.S.C. § 102(e) - Purtell

The Office at 5 states:

As to claim 10, Purtell et al discloses using Internet Protocol (IP) [column 3 line 51 to column 4 line 11].

As amended, Applicant's independent claim 1 now recites a limitation wherein the second connection is different than the first connection and the third connection is different than the second connection and the first connection upon which dependent claim 10 depends. Applicant submits that because Purtell fails to disclose a second and third connections that are each different, that Purtell fails to anticipate what Applicant has claimed. Applicant respectfully requests allowance of dependent claim 10.

The additional limitation in claim 10 is also not anticipated. Applicant respectfully requests allowance of claim 10.

Claim 12 Rejection under 35 U.S.C. § 102(e) - Purtell

The Office at 5 states:

As to claim 12, Purtell et al discloses using Ethernet with the Transmission Control Protocol (TCP) [column 3 line 51 to column 4 line 11].

As amended, Applicant's independent claim 1 now recites a limitation wherein the second connection is different than the first connection and the third connection is different than the second connection and the first connection upon which dependent claim 12 depends. Applicant submits that because Purtell fails to disclose a second and third connections that are each different, that Purtell fails to anticipate what Applicant has claimed. Applicant respectfully requests allowance of dependent claim 12.

The additional limitation in claim 12 is also not anticipated. Applicant respectfully requests allowance of claim 12.

Claims Rejection under 35 U.S.C. § 102(b) - Freund

The Office at 6 states:

6. Claims 17-21 are rejected under 35 U.S.C. 102(b) as being anticipated by Freund U.S. Patent No. 5,987,611.
(Emphasis in original.)

Claim 17 Rejection under 35 U.S.C. § 102(b) - Freund

The Office at 6 states:

As to claim 17, Freund discloses a firewall traversal system comprising:

a main system coupled to storage [column 14 line 52 to column 15 line 11];

a communication subsystem coupled to the main system and a communication medium on one side of a firewall [column 5, lines 9-27];

a packet examining subsystem coupled to the communication subsystem [column 5, lines 34-50]; and

a database system coupled to the packet examining subsystem and the main system [column 6, lines 13-27].

The cited reference [column 14 line 52 to column 15 line 11] states:

FIG. 3A provides an overview of an Internet-based (client/server) system 300 in which the present invention may be embodied. As shown, the system includes multiple clients 310 (e.g., clients 310a, 310b, 310c, each of which comprises a personal computer or workstation, such as system 100) connected to a network 320, such as a Windows NT Local Area Network (Microsoft Corporation of Redmond, Wash.). Each client includes a client-side monitoring component for monitoring Internet access in accordance with the present invention, as specifically shown at 311a, 311b, and 311c. The network 320 is connected to a server 321 (or another client) having a supervisor or verifier component 323. The supervisor component 323 provides independent verification of the clients, for allowing or disallowing requests of each particular client. In effect, the supervisor 323 directs runtime monitoring operations.

The network 320 itself can be a server-based network (e.g., Windows NT Server providing services to network clients) or, alternatively, a peer-to-peer network. Communications to the outside (e.g., Internet) are typically achieved using TCP/IP protocol. The local network 320 communicates with the Internet, shown at 340, preferably through a "firewall" 330. The firewall 330 itself may be implemented in a conventional manner, such as employing a router-based or server-based firewall process for monitoring communications with various Web servers 350 connected to the Internet 340.

Firstly, Freund Figure 3A shows Clients 310, LAN 320, Server 321, Firewall 330, Internet 340, and Web servers 350. Nowhere in Figure 3A does Freund disclose "a main system coupled to storage" as Applicant has claimed.

The cited reference [column 5, lines 9-27] states in part:

The centralized supervisor application is installed on a computer on the LAN that can be reached from all workstations that need access to the Internet; this is typically (although not necessarily) a server computer. The supervisor monitors whether a client has the filter application loaded and provides the filter application with the rules for the specific user or workstation. The filter application maintains a local copy of these rules so that rule enforcement continues even when the user accesses the Internet but bypasses the LAN (e.g., a mobile computer on the road). The communication between the client-based filter and the centralized supervisor application, as well as between the supervisor application and the firewall, employs encryption to ensure secure communication and avoid any possible attack on that level.

The system of the present invention works together with existing firewalls which allow a program (e g , the supervisor application) to dynamically set the addresses of the workstations that should have access to the Internet. The supervisor application signals the firewall which client applications have been "certified" so that the firewall only grants Internet access to those clients. At the same time, a firewall can continue to perform its usual duties, such as protecting the LAN from outside intruders or protecting the LAN and server operating system(s).

Secondly, Freund here is discussing a centralized supervisor application with rules and enforcement with computers attached via a server, and updates to a firewall on client applications that have been "certified." Freund does not disclose "a communication subsystem coupled to the main system and a communication medium on one side of a firewall" as Applicant has claimed.

The cited reference [column 5, lines 34-50] states:

1. Client Monitor with Supervisor/Firewall Backup and Enforcement

a) Installing at a particular client computer a client monitoring process;

b) Installing at another computer on the local area network a supervisor process, which specifies rules which govern Internet access by the client computers including the particular client computer;

c) Transmitting a filtered subset of the rules to the particular client computer;

d) At the client monitoring process, trapping a request for Internet access from the particular client computer;

e) Determining whether the request for Internet access would violate any of the rules transmitted to the particular client computer, and

f) If the request for Internet access violates any of the rules transmitted to the particular client computer, denying the request for Internet access.

Thirdly, Freund here is discussing "at a particular client computer a client monitoring process" and "at another computer on the local area network a supervisor process" and the monitoring process "trapping a request for Internet access". Trapping a request for Internet access is different than "a packet examining subsystem coupled to the communication subsystem" as Applicant has claimed, because trapping (Freund) is not the same as examining a packet (Applicant).

The cited reference [column 6, lines 13-27] states in part:

IV. Monitoring User Interaction (e.g., keyboard/mouse and the like) to Distinguish and Regulate Time Spent Online:

a) Client Monitor detects interactive commands (e.g., keyboard/mouse) for an application that uses the Internet via "browsing" protocols (e.g., HTTP).

b) Client monitor determines whether the user interactively uses the Internet and restrict the activity if required.

V. Using Client Monitor to Alleviate Network Congestion

a) Supervisor Application notifies client that network is congested; and

b) Client Monitor delays transmission of non-time critical information and data.

VI. Using Local and Remote Stored Rules Databases to Allow Client Monitor Functioning Even if Supervisor Application is Not Available

a) Client monitor attempts but is unable to access the supervisor application; and

b) Access rules are still enforced because Client Monitor employs a local copy of rules (previously downloaded).

Fourthly, nowhere in this cited section does Freund discuss or disclose "a database system coupled to the packet examining subsystem and the main system" as Applicant has claimed.

Applicant submits that for the above four reasons individually and/or in combination, Freund fails to disclose what Applicant has claimed in independent claim 17. Applicant respectfully requests allowance of claim 17 and claims 18-21 which are dependent on claim 17.

Claim 18 Rejection under 35 U.S.C. § 102(b) - Freund

The Office at 6 states:

As to claim 18, Freund discloses that the packet examining subsystem extracts port information [column 16, lines 8-29].

Claim 18 is dependent on claim 17, and as detailed above in the claim 17 discussion, Freund does not anticipate Applicant's independent claim 17. The additional limitation in claim 18 is thus also not anticipated. Applicant respectfully requests allowance of claim 18 and further dependent claim 19.

Claim 19 Rejection under 35 U.S.C. § 102(b) - Freund

The Office at 6 states:

> As to claim 19, Freund discloses that the packet examining subsystem extracts the port information based upon examining packet data content [column 16, lines 8-29].

Claim 19 is dependent on claim 18, which is dependent on claim 17, and as detailed above in the claim 17 discussion, Freund does not anticipate Applicant's independent claim 17. The additional limitation in claim 19 is thus also not anticipated. Applicant respectfully requests allowance of claim 19.

Claim 20 Rejection under 35 U.S.C. § 102(b) - Freund

The Office at 6 states:

> As to claim 20, Freund discloses that the packet examining subsystem extracts address information [column 13, lines 34-43].

Claim 20 is dependent on claim 17, and as detailed above in the claim 17 discussion, Freund does not anticipate Applicant's independent claim 17. The additional limitation in claim 20 is thus also not anticipated. Applicant respectfully requests allowance of claim 20 and further dependent claim 21.

Claim 21 Rejection under 35 U.S.C. § 102(b) - Freund

The Office at 6 states:

As to claim 21, Freund discloses that the packet examining subsystem extracts the address information based upon examining packet data content [column 13, lines 34-43].

Claim 21 is dependent on claim 20, which is dependent on claim 17, and as detailed above in the claim 17 discussion, Freund does not anticipate Applicant's independent claim 17. The additional limitation in claim 21 is thus also not anticipated. Applicant respectfully requests allowance of claim 21.

Claim 4 Rejection under 35 U.S.C. § 103(a) – Purtell in view of Bhide

The Office at 7 states:

7. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Purtell et al U.S. Patent No. 6,950,947 B1 as applied to claim 1 above, and further in view of Bhide et al U.S. Patent No. 5,852,717.
(Emphasis in original.)

As to claim 4, Purtell et al does not teach initiating a HTTP connection that comprises initiating a HTTP connection to a predefined address using port 80.

Bhide et al teaches initiating a HTTP connection that comprises initiating a HTTP connection to a predefined address using port 80 [column 5, lines 9-21].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Purtell et al so that if a HTTP connection were to initiate between a client and server, it would have used a predefined address using port 80.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Purtell et al by the teaching of Bhide et al because it is well known in the art that a HTTP connection uses port 80. Establishing a connection involves one round-trip time from the client to the server as the client requests to open a network connection and the server responds that a network connection has been opened [column 5, lines 9-21].

Claim 4 is dependent on claim 2, which is dependent on claim 1. The issue of a 102(e) Purtell rejection for claim 1 is addressed above and incorporated herein. As discussed above, Applicant's amended independent claim 1 now recites a limitation wherein the second connection is different than the first connection and the third connection is different than the second connection and the first connection upon which dependent claim 4 depends. Purtell fails to disclose a second and third connections that are each different. Bhide et al ("Bhide") also fails to disclose a second and third connections that are each different. Purtell in view of Bhide also fails to disclose Applicant's limitation wherein the second connection is different than the first connection and the third connection is different than the second connection and the first connection. Applicant respectfully requests allowance of claim 4.

Claims 5-9 Rejection under 35 U.S.C. § 103(a) – Purtell in view of Fuh

The Office at 8 states:

8. Claims 5-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Purtell et al U.S. Patent No. 6,950,947 B1 as applied to claim 1 above, and further in view of Fuh et al U.S. Patent No. 6,609,154 B1.
(Emphasis in original.)

Claims 5-7, and 9 Rejection under 35 U.S.C. § 103(a) – Purtell in view of Fuh

The Office at 8 states:

As to claims 5-7 and 9, Purtell et al does not teach that initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address and port. Purtell et al does not teach that determining a likely proxy address and port further comprises packet sniffing. Purtell et al does not teach that packet sniffing further comprises: sampling packets; extracting information from the sampled packets; and building a database of likely proxy addresses and ports. Purtell et at does not teach that extracting information from the sampled packets comprises examining TCP packets for HTTP data.

Fuh et al teaches initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address and port [column 13, lines 3-14]. **[Claim 5]**

Fuh et al teaches that determining a likely proxy address and port further comprises packet sniffing [column 9, lines 51-67]. **[Claim 6]**

Fuh et al teaches that packet sniffing further comprises: sampling packets; extracting information from the sampled packets; and building a database of likely proxy addresses and ports [column 9, lines 51-67]. **[Claim 7]**

Fuh et al teaches that extracting information from the sampled packets comprises examining TCP packets for HTTP data [column 9, lines 51-67]. **[Claim 9]**

[Bracketed bolded added for ease of discussion]

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Purtell et al so that there would have been a HTTP connection initiated via a proxy connection that would have determined a likely proxy address and port. Packet sniffing would have occurred during the determining step of the proxy address and port. The firewall packet sniffing would have included sampling packets, extracting information from the packets and building a database of likely proxy addresses and ports. The extracted information would have come from examining TCP packets for HTTP data.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Purtell et al by the teaching of Fuh et al because it makes sure that the client is authorized to communicate with a network resource [column 3, lines 54-60].

The cited reference states in part:

[column 13, lines 3-14]

As shown in block 738, the process waits. For example, after Authentication Proxy 400 sends the "Authentication Success" message 524 to User 302, the Authentication Proxy enters a wait state for a short, pre-determined period of time. During the wait state, a short period of time is allowed to elapse to enable client 306 and firewall router 210 to communicate handshaking messages and carry out related processing associated with establishing an HTTP connection.

The delay period also allows the firewall router enough time to execute any commands that are issued as part of block 734. In one embodiment, a period of three (3) seconds elapses.

[column 9, lines 51-67]

Access control lists filter packets and can prevent certain packets from entering or exiting a network. Each ACL is a list of information that firewall router 210 may use to determine whether packets arriving at or sent from a particular interface may be communicated within or outside the firewall router. For example, in an embodiment, input ACL 424 may comprise a list of IP addresses and types of allowable client protocols. Assume that firewall router 210 receives an inbound packet from client 306 at external interface 420 that is intended for target server 222. If the IP address of client 306 is not stored in input ACL 424, then firewall router 210 will not forward the packet further within the circuitry or software of the firewall router. Output ACL 426 similarly controls the delivery of packets from firewall router 210 to resources located outside external interface 420. Input ACL 428 and output ACL 430 govern packet flow to or from internal interface 422.

[column 3, lines 54-60].

In another feature, determining whether the client is authorized to communicate with the network resource comprises the steps of determining whether a source IP address of the client in the request matches information in a filtering mechanism of the network device, and if so, determining whether the source IP address matches the authorization information stored in the network device.

Applicant's claims 5-7 and 9 recite:

5. (original) The method according to claim 2, wherein initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address and port.

6. (original) The method according to claim 5, wherein determining a likely proxy address and port further comprises packet sniffing.

7. (original) The method according to claim 6, wherein packet sniffing further comprises:

sampling packets;

extracting information from the sampled packets; and

building a database of likely proxy addresses and ports.

9. (original) The method according to claim 7, wherein extracting information from the sampled packets comprises examining TCP packets for HTTP data.

Firstly, claims 5-7, and 9 are dependent on claim 2, which is dependent on claim 1. The issue of a 102(e) Purtell rejection for claim 1 is addressed above and incorporated herein. As discussed above, Applicant's amended independent claim 1 now recites a limitation wherein the second connection is different than the first connection and the third connection is different than the second connection and the first connection upon which dependent claims 5-7, and 9 depend. Purtell fails to disclose a second and third connections that are each different. Fuh et al ("Fuh") also fails to disclose a second and third connections that are each different. Purtell in view of Fuh also fails to disclose Applicant's limitation wherein the second connection is different than the first connection and the third connection is different than the second connection and the first connection. Applicant respectfully requests allowance of claims 5-7, and 9.

Specifically with respect to claim 5

Applicant's claim 5 recites:

5. (original) The method according to claim 2, wherein initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address and port.
[Emphasis added.]

Applicant's claim 5 is dependent on claim 2, which is in turn dependent on claim 1. The issue of a 102(e) Purtell rejection for claims 1, and 2 are addressed above and incorporated herein.

Applicant submits that Fuh is fundamentally different than Applicant's claim 5. While Applicant teaches determining a likely proxy address and port, Fuh (see Abstract) on the other hand teaches "network access control" and "intercept network traffic." Further, Fuh Figure 2 at 210 clearly shows intercepting traffic to/from 206 and 216 and the specification details authentication based on AA server 218 and Database

220. Network access control and intercepting network traffic (Fuh) is not the same as determining a likely proxy address and port (Applicant's claim 5)

Additionally, while the Office states "Fuh et al teaches initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address and port [column 13, lines 3-14]." Applicant submits that the cited lines discuss the authentication process and do not teach anything about determining a like proxy address and port as in Applicant's claim 5.

Finally, modifying Purtell with Fuh does not disclose or make obvious the "firewall" aspect of claim 1 or the "determining a likely proxy address and port" aspect of claim 5. Applicant respectfully requests removal of this rejection for claim 5 and claims 6-9 which are dependent on claim 5.

Specifically with respect to claim 6

Applicant's claim 6 recites:

6. (original) The method according to claim 5, wherein determining a likely proxy address and port further comprises packet sniffing.

[Emphasis added.]

The Office cites Fuh for "Fuh et al teaches that determining a likely proxy address and port further comprises packet sniffing [column 9, lines 51-67]."

Applicant submits that Fuh actually teaches away from Applicant's claim 6. While Applicant teaches sniffing packets which does not involve altering in any way the communication, Fuh (see Abstract) on the other hand teaches network access control and intercepting network traffic. Intercepting network traffic (Fuh) is the *antithesis* of packet sniffing (Applicant).

Further, Applicant submits that the cited lines discuss the Authentication and Authorization process and do not teach anything about determining a likely proxy address and port further comprises packet sniffing as in Applicant's claim 6. Fuh at the lines cited

specifically says "Access control lists filter packets .... If the IP address of client 306 is not stored in input ACL 424, then firewall router 210 will not forward the packet further within the circuitry or software of the firewall router. Output ACL 426 similarly controls the delivery of packets from firewall router 210 to resources located outside external interface 420."

[Emphases added.]

Fuh teaches away from packet sniffing and deals with filtering packets, not forwarding packets, and controlling delivery.

Finally, modifying Purtell with Fuh does not disclose or make obvious the "packet sniffing" aspect of claim 6. Applicant respectfully requests removal of this rejection for claim 6 and claims 7-9 which are dependent on claim 6.

Specifically with respect to claim 7

Applicant's claim 7 recites:

7. (original) The method according to claim 6, wherein packet sniffing further comprises:

sampling packets;

extracting information from the sampled packets; and

building a database of likely proxy addresses and ports.

The Office cites Fuh for "Fuh et al teaches that packet sniffing further comprises: sampling packets; extracting information from the sampled packets; and building a database of likely proxy addresses and ports [column 9, lines 51-67]."

Applicant submits that the cited lines discuss the Authentication and Authorization process and do not teach anything about sampling packets; extracting information from the sampled packets; and building a database of likely proxy addresses and ports as in Applicant's claim 7.

Fuh at the lines cited specifically says "Access control lists filter packets .... If the IP address of client 306 is not stored in input ACL 424, then firewall router 210 will not forward the packet further within the circuitry or software of the firewall router. Output ACL 426 similarly controls the delivery of packets from firewall router 210 to resources located outside external interface 420."

[Emphases added.]

As discussed above for claim 6, Fuh teaches away from packet sniffing and deals with filtering packets, not forwarding packets, and controlling delivery.

Finally, modifying Purtell with Fuh does not disclose or make obvious the "sampling packets; extracting information from the sampled packets; and building a database of likely proxy addresses and ports" aspect of claim 7. Applicant respectfully requests removal of this rejection for claim 7 and claims 8-9 which are dependent on claim 7.

Claim 8 Rejection under 35 U.S.C. § 103(a) – Purtell in view of Fuh

The Office at 8 states:

As to claim 8, Purtell et al teaches that extracting information from the sampled packets comprises extracting TCP port information [column 1 line 50 to column 2 line 3].

The cited reference states in part:

Several authentication and authorization mechanisms are suitable for use with operating systems that are used by network devices, such as the Internetworking Operating System ("IOS") commercially available from Cisco Systems, Inc. However, most prior authentication and authorization mechanisms are associated with dial-up interfaces, which can create network security problems. In a dial-up configuration, a remote client uses a telephone line and modem to dial up a compatible modem that is coupled to a server of the network that the remote client wishes to access. In another dial-up configuration, a remote client first establishes a dial-up connection to a server associated with an Internet Service

Provider, and that server then connects to the network server through the global, public, packet-switched internetwork known as the Internet. In this configuration, the network server is coupled directly or indirectly to the Internet.

Unfortunately, information requests and other traffic directed at a network server from the Internet is normally considered risky, untrusted traffic. An organization that owns or operates a network server can protect itself from unauthorized users or from unwanted traffic from the Internet by using a firewall. . .

Applicant's claim 8 recites:

8. (original) The method according to claim 7, wherein extracting information from the sampled packets comprises extracting TCP port information.

Claim 8 is dependent on claim 7, which is dependent on claim 6, which is dependent on claim 5, which is dependent on claim 2, which is dependent on claim 1. The issue of a 102(e) Purtell rejection for claim 1 is addressed above and incorporated herein.

Applicant submits that nowhere in the cited section does Fuh mention what Applicant has claimed. Furthermore, nowhere does Fuh mention "extracting" TCP port information from sampled packets. Finally, modifying Purtell with Fuh does not disclose or make obvious "wherein extracting information from the sampled packets comprises extracting TCP port information" limitation of claim 8. Applicant respectfully requests removal of this rejection for claim 8, and allowance of claim 8.

Claims 11 and 13 Rejection under 35 U.S.C. § 103(a) – Purtell in view of Fuh

The Office at 9 states:

9. Claims 11 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Purtell et al U.S. Patent No. 6,950,947 B1 as applied to claim 1 above, and further in view of Fuh et al U.S. Patent No. 6,609,154 B1.

(Emphasis in original.)

As to claims 11 and 13, Purtell et al does not teach that initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address by sampling packets and extracting IP and Ethernet addresses.

Fuh et al teaches initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address by sampling packets and extracting IP and Ethernet addresses **[column 9, lines 51-67].**

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Purtell et al so that a HTTP connection would have been initiated via a proxy connection and proxy addresses would have been determined by sampling packets and extracting IP and Ethernet address.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Purtell et al by the teaching of Fuh et al because it makes sure that the client is authorized to communicate with a network resource **[column 3, lines 54-60].**

(Emphases added.)

The cited reference states in part:

[column 9, lines 51-67]

Access control lists filter packets and can prevent certain packets from entering or exiting a network. Each ACL is a list of information that firewall router 210 may use to determine whether packets arriving at or sent from a particular interface may be communicated within or outside the firewall router. For example, in an embodiment, input ACL 424 may comprise a list of IP addresses and types of allowable client protocols. Assume that firewall router 210 receives an inbound packet from client 306 at external interface 420 that is intended for target server 222. If the IP address of client 306 is not stored in input ACL 424, then firewall router 210 will not forward the packet further within the circuitry or software of the firewall router. Output ACL 426 similarly controls the delivery of packets from firewall router 210 to resources located outside external interface 420. Input ACL 428 and output ACL 430 govern packet flow to or from internal interface 422.

[column 3, lines 54-60]

In another feature, determining whether the client is authorized to communicate with the network resource comprises the steps of: determining whether a source IP address of the client in the request matches information in a filtering mechanism of the network device; and if so, determining whether the source IP address matches the authorization information stored in the network device.

Specifically with respect to claim 11

Applicant's claims 11 recites:

11. (original) The method according to claim 10, wherein initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address by sampling packets and extracting IP addresses.

As detailed above, Applicant submits that the cited lines discuss the Authentication and Authorization process and do not teach anything about determining a likely proxy address by sampling packets and extracting IP addresses as in Applicant's claim 11. Fuh at the lines cited specifically says "Access control lists filter packets .... If the IP address of client 306 is not stored in input ACL 424, then firewall router 210 will not forward the packet further within the circuitry or software of the firewall router. Output ACL 426 similarly controls the delivery of packets from firewall router 210 to resources located outside external interface 420."

[Emphases added.]

Filtering packets and not forwarding packets (Fuh) is not the same as sampling packets or extracting IP addresses (as in Applicant's claim 11).

Finally, modifying Purtell with Fuh does not disclose or make obvious the "determining a likely proxy address by sampling packets and extracting IP addresses" aspect of claim 11. Applicant respectfully requests removal of this rejection for claim 11.

Specifically with respect to claim 13

Applicant's claim 13 recites:

13. (original) The method according to claim 12, wherein initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address by sampling packets and extracting Ethernet addresses.

As detailed above, Applicant submits that the cited lines discuss the Authentication and Authorization process and do not teach anything about determining a likely proxy address by sampling packets and extracting Ethernet addresses as in Applicant's claim 13.

Fuh at the lines cited specifically says "Access control lists filter packets .... If the IP address of client 306 is not stored in input ACL 424, then firewall router 210 will not forward the packet further within the circuitry or software of the firewall router. Output ACL 426 similarly controls the delivery of packets from firewall router 210 to resources located outside external interface 420."

[Emphases added.]

Filtering packets and not forwarding packets (Fuh) is not the same as sampling packets or extracting Ethernet addresses (as in Applicant's claim 13).

Finally, modifying Purtell with Fuh does not disclose or make obvious the "determining a likely proxy address by sampling packets and extracting Ethernet addresses" aspect of claim 13. Applicant respectfully requests removal of this rejection for claim 13.

Claim 16 Rejection under 35 U.S.C. § 103(a) – Purtell in view of Linden

Applicant's claim 16 recites:

16. (original) The machine-readable medium according to claim 15, further configuring said processor to perform the following:

examine network traffic; and

build a database of parameters likely to allow establishment of a HTTP connection via a proxy connection.

The Office at 10 states:

10. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Purtell et al U.S. Patent No. 6,950,947 B1 as applied to claim 14 above, and further in view of Linden et al U.S. Patent No. 6,549,773 B1.
(Emphasis in original.)

As to claim 16, Purtell et al teaches examining network traffic **[column 5, lines 47-67]**.

Purtell et al does not teach building a database of parameters likely to allow establishment of a HTTP connection via a proxy connection.

Linden et al teaches building a database of parameters likely to allow establishment of a HTTP connection via a proxy connection **[column 5, lines 16-26]**.

Therefore, it would have been obvious ...

(Emphases added.)

The cited reference states in part:

[column 5, lines 47-67] - PURTELL

A firewall 100 may share CCBs 300 with another firewall 100 on the internal network by pushing its own CCBs 300 to one or more network peers, or by pulling CCBs 300 from one or more network peers. If the firewall 100 pushes its CCBs 300 to a network peer, the firewall 100 makes a copy of the one or more CCBs 300 associated with its TCP connections, and transmits those CCBs 300 to one or more other firewalls 100 in a CCB update packet 400. In a preferred embodiment, the firewall 100 pushes a CCB update packet 400 to its network peers on a periodic basis, that period is preferably fixed and preferably chosen to be within the range of one second to thirty seconds. A thirty-second period is advantageously utilized. Of course, the period may be less than one second or more than thirty seconds, depending on the speed of the internal network 102 and the firewalls 102, and the network conditions on the internal network 102. It is also contemplated that the period between transmission of CCB update packets 400 need not be fixed, but may vary depending on network conditions and on network traffic through the firewalls 100 between the internal network 102 and the external network 104. It is also within the scope of the preferred embodiment to issue a CCB update packet 400 from a firewall 100 only after the firewall 100 makes a new TCP connection, thus allowing the firewall 100 to provide highly current network state data to its peers.

Applicant submits that the cited lines in Purtell discuss the movement and updating of control blocks (CCB) and do not teach anything about *examining* network traffic as in Applicant's claim 16.

[column 5, lines 16-26]- LINDEN

A particular advantage of the invention e.g. in connection with the WAP application protocol is that it is possible to efficiently utilize functions connected with the HTTP data transmission protocol of the WSP/B protocol already known as such. These include, for example, GET, PUT, and POST requests. Consequently, the header fields of

the HTTP protocol can also be utilized in the data transmission, as well as the headers of the HTTP protocol for authentication. Correspondingly, it is possible to utilize efficiently the methods of the WWW communication network for authorization or data transmission.

Applicant submits that the cited lines of Linden et al ("Linden") discuss protocols and do not teach anything about building a database of parameters likely to allow establishment of a HTTP connection via a proxy connection as in Applicant's claim 16.

Applicant submits that Purtell in view of Linden does not make obvious what is in Applicant's claim 16. Applicant therefore respectfully requests removal of this rejection for claim 16.

Claims 24 and 25 under 35 U.S.C. § 103(a) – Purtell in view of Fuh

The Office at 11 states:

11. Claims 24 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Purtell et al U.S. Patent No. 6,950,947 B1 as applied to claim 22 above, and further in view of Fuh et al U.S. Patent No. 6,609,154 B1.

(Emphasis in original.)

As to claims 24 and 25, Purtell et al does not teach means for initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address by sniffing packets and extracting information from the packets. Purtell et al does not teach means for initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address by receiving information from a computer connected to the firewall.

Fuh teaches means for initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address by sniffing packets and extracting information from the packets **[column 9, lines 51-67]**. Fuh teaches means for initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address by receiving information from a computer connected to the firewall [column 9, lines 51-67].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Purtell et al so that a HTTP connection would have been initiated via a proxy connection. The firewall would have sniffed packets and extracted information from the packets. Proxy addresses would have been determined by receiving information from the computer connected to the firewall.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Purtell et al by the teaching of Fuh et al because it makes sure that the client is authorized to communicate with a network resource **[column 3, lines 54-60]**.

(Emphases added.)

The cited reference states in part:

[column 9, lines 51-67]

Access control lists filter packets and can prevent certain packets from entering or exiting a network. Each ACL is a list of information that firewall router 210 may use to determine whether packets arriving at or sent from a particular interface may be communicated within or outside the firewall router. For example, in an embodiment, input ACL 424 may comprise a list of IP addresses and types of allowable client protocols. Assume that firewall router 210 receives an inbound packet from client 306 at external interface 420 that is intended for target server 222. If the IP address of client 306 is not stored in input ACL 424, then firewall router 210 will not forward the packet further within the circuitry or software of the firewall router. Output ACL 426 similarly controls the delivery of packets from firewall router 210 to resources located outside external interface 420. Input ACL 428 and output ACL 430 govern packet flow to or from internal interface 422.

[column 3, lines 54-60]

In another feature, determining whether the client is authorized to communicate with the network resource comprises the steps of: determining whether a source IP address of the client in the request matches information in a filtering mechanism of the network device; and if so, determining whether the source IP address matches the authorization information stored in the network device

Specifically with respect to claim 24

Applicant's claim 24 recites:

24. (original) The apparatus of claim 23, wherein means for initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address by sniffing packets and extracting information from the packets.
[Emphasis added.]

Applicant submits that Fuh actually teaches away from Applicant's claim 24. While Applicant teaches sniffing packets which does not involve altering in any way the communication, Fuh (see Abstract) on the other hand teaches network access control and intercepting network traffic. Intercepting network traffic (Fuh) is the *antithesis* of packet sniffing (Applicant).

Further, Applicant submits that the cited lines discuss the Authentication and Authorization process and do not teach anything about determining a likely proxy address by sniffing packets and extracting information from the packets as in Applicant's claim 24.

Fuh at the lines cited specifically says "Access control lists filter packets .... If the IP address of client 306 is not stored in input ACL 424, then firewall router 210 will not forward the packet further within the circuitry or software of the firewall router. Output ACL 426 similarly controls the delivery of packets from firewall router 210 to resources located outside external interface 420."

[Emphases added.]

Fuh teaches away from packet sniffing and deals with filtering packets, not forwarding packets, and controlling delivery.

Claim 24 is dependent on claim 23, which is dependent on claim 22. The issue of a 102(e) Purtell rejection for claim 22 is addressed above and incorporated herein. As discussed above Applicant's amended independent claim 22 now recites a limitation wherein the second connection is different than the first connection and the third connection is different than the second connection and the first connection upon which

dependent claim 24 depends. Fuh fails to disclose a second and third connections that are each different. Fuh also fails to disclose a second and third connections that are each different. Purtell in view of Fuh also fails to disclose Applicant's limitation wherein the second connection is different than the first connection and the third connection is different than the second connection and the first connection. Applicant respectfully requests allowance of claim 24.

Finally, modifying Purtell with Fuh does not disclose or make obvious the "packet sniffing" aspect of claim 24. Applicant respectfully requests removal of this rejection for claim 24.

Specifically with respect to claim 25

Applicant's claim 25 recites:

25. (original) The apparatus of claim 23, wherein means for initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address by receiving information from a computer connected to the firewall.

[Emphasis added.]

The Office (page 9, paragraph 11) states:

Fuh teaches means for initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address by receiving information from a computer connected to the firewall [column 9, lines 51-67].

Applicant submits that the cited lines discuss the Authentication and Authorization process and do not teach anything about determining a likely proxy address by receiving information from a computer connected to the firewall as in Applicant's claim 25.

Fuh at the lines cited specifically says "Access control lists filter packets .... If the IP address of client 306 is not stored in input ACL 424, then firewall router 210 will not forward the packet further within the circuitry or software of the firewall router. Output ACL 426 similarly controls the delivery of packets from firewall router 210 to resources located outside external interface 420."

[Emphases added.]

Claim 25 is dependent on claim 23, which is dependent on claim 22. The issue of a 102(e) Purtell rejection for claim 22 is addressed above and incorporated herein. As discussed above, Applicant's amended independent claim 22 now recites a limitation wherein the second connection is different than the first connection and the third connection is different than the second connection and the first connection upon which dependent claim 25 depends. Fuh fails to disclose a second and third connections that are each different. Fuh also fails to disclose a second and third connections that are each different. Purtell in view of Fuh also fails to disclose Applicant's limitation wherein the second connection is different than the first connection and the third connection is different than the second connection and the first connection. Applicant respectfully requests allowance of claim 25.

Finally, modifying Purtell with Fuh does not disclose or make obvious the "receiving information from a computer connected to the firewall" aspect of claim 25. Applicant respectfully requests removal of this rejection for claim 25.

Claim 26 under 35 U.S.C. § 103(a) – Purtell in view of Montenegro

The Office at 12 states:

12. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Purtell et al U.S. Patent No. 6,950,947 131 as applied to claim 22 above, and further in view of Montenegro U.S. Patent No. 6,233,688 B1.

(Emphasis in original.)

As to **claim 26**, Purtell et al does not teach means for updating firewall traversal strategies.

Montenegro teaches means for updating firewall traversal strategies **[column 6, lines 49-65]**.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Purtell et al so that there would have been a firewall that had means for updated firewall traversal strategies.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Purtell et al by the teaching of Montenegro because it keeps the firewall up to date as far as addressed to block so that the client is not compromised at any time **[column 2, lines 7-21]**.

(Emphasis added.)

The cited reference states:

[column 6, lines 49-65]

The first step in creating a transparency between the firewall traversal for remote access and the client application is to obtain the appropriate RAFT URL (step S10). The discovery of the specific RAFT URL to use is not a subject of the essential invention. Obtaining a RAFT URL may be achieved in several ways: (1) obtaining it in person from a system administrator, (2) visiting a special web page where an authenticated user may retrieve the appropriate RAFT URL from the firewall, (3) querying a directory service such as LDAP (Lightweight Directory Access Protocol) or (4) may be preconfigured into the client application or system. The appropriate RAFT URL will designate parameters allowing the client system to get private intranet resources through its data transport mechanisms (IP stack, sockets, etc.)

(Emphases added.)

[column 2, lines 7-21]

The invention provides a generic naming scheme for remote access and firewall traversal in the form of a uniform resource locator (RAFT URL). The RAFT URL may be provided to any client application, regardless of compatibility with the remote access/firewall traversal method, which then launches another executable module. The executable module performs the remote access/firewall traversal method and interacts with the operating environment to obtain data transport mechanisms. These mechanisms permit the client application to transact with private resources beyond the firewall. The remote access/firewall traversal procedure is made transparent to the client application, and thus, a wider array of client applications may be chosen for the data session with the resources beyond the firewall

(Emphases added.)

Applicant's claim 26 recites:

26. (original) The apparatus of claim 22, further comprising means for updating firewall traversal strategies.

Applicant submits that Montenegro does not teach `"means for updating firewall traversal strategies"`. To the contrary at the cited reference lines Montenegro assumes that a RAFT URL exists (The RAFT URL may be provided to any client application) and then uses this to launch an executable to get through a firewall (The executable module performs the remote access/firewall traversal method). Montenegro does not disclose a means for "updating firewall traversal strategies" as Applicant has claimed.

Claim 26 is dependent on claim 22. The issue of a 102(e) Purtell rejection for claim 22 is addressed above and incorporated herein. As discussed above Applicant's amended independent claim 22 now recites a limitation wherein the second connection is different than the first connection and the third connection is different than the second connection and the first connection upon which dependent claim 26 depends. Montenegro fails to disclose a second and third connections that are each different. Montenegro also fails to disclose a second and third connections that are each different. Purtell in view of Montenegro also fails to disclose Applicant's limitation wherein the second connection is

different than the first connection and the third connection is different than the second connection and the first connection. Applicant respectfully requests allowance of claim 26.

Finally, modifying Purtell with Montenegro does not disclose or make obvious "means for updating firewall traversal strategies" aspect of claim 26. Applicant respectfully requests removal of this rejection for claim 26.

CONCLUSION

Applicant submits that the rejection of dependent claims not specifically addressed, are addressed by Applicant's arguments to the claim(s) on which they depend.

Applicant respectfully submits that all claims are in condition for allowance and request such.

Communication via cleartext email is authorized.

Respectfully submitted,

Heimlich Law

07/24/2006

Digitally signed by Alan Heimlich
DN: CN = Alan Heimlich, C = US O = Heimlich Law

Date

Alan Heimlich / Reg 48808

Attorney for Applicant(s)

Customer No. 40418

5952 Dial Way
San Jose, CA 95129

Tel: 408 253-3860
Eml: alanheimlich@heimlichlaw.com